

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»»

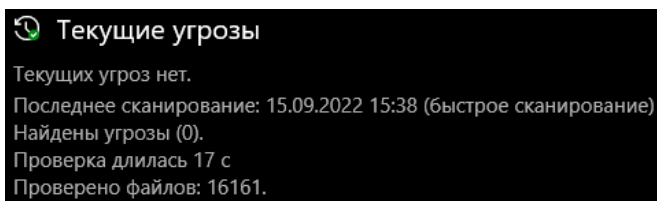
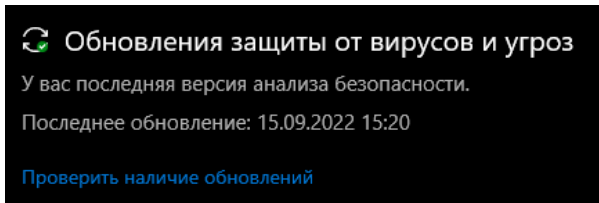
ЛАБОРАТОРНАЯ РАБОТА №1:
«Антивирусное ПО»

Выполнили студенты группы Б19-515
Щербакова Александра
Белов Александр

Москва, 2022 г.

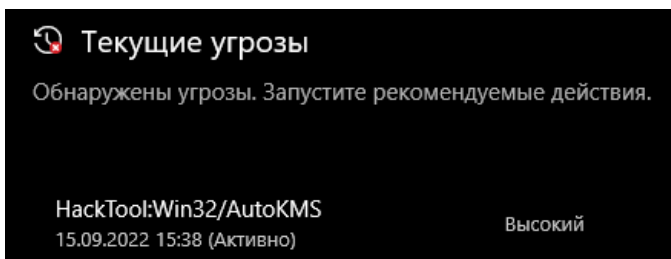
1. Microsoft Defender

1.1 Вирусные базы обновлены, при быстрой проверке системы угроз не обнаружено.



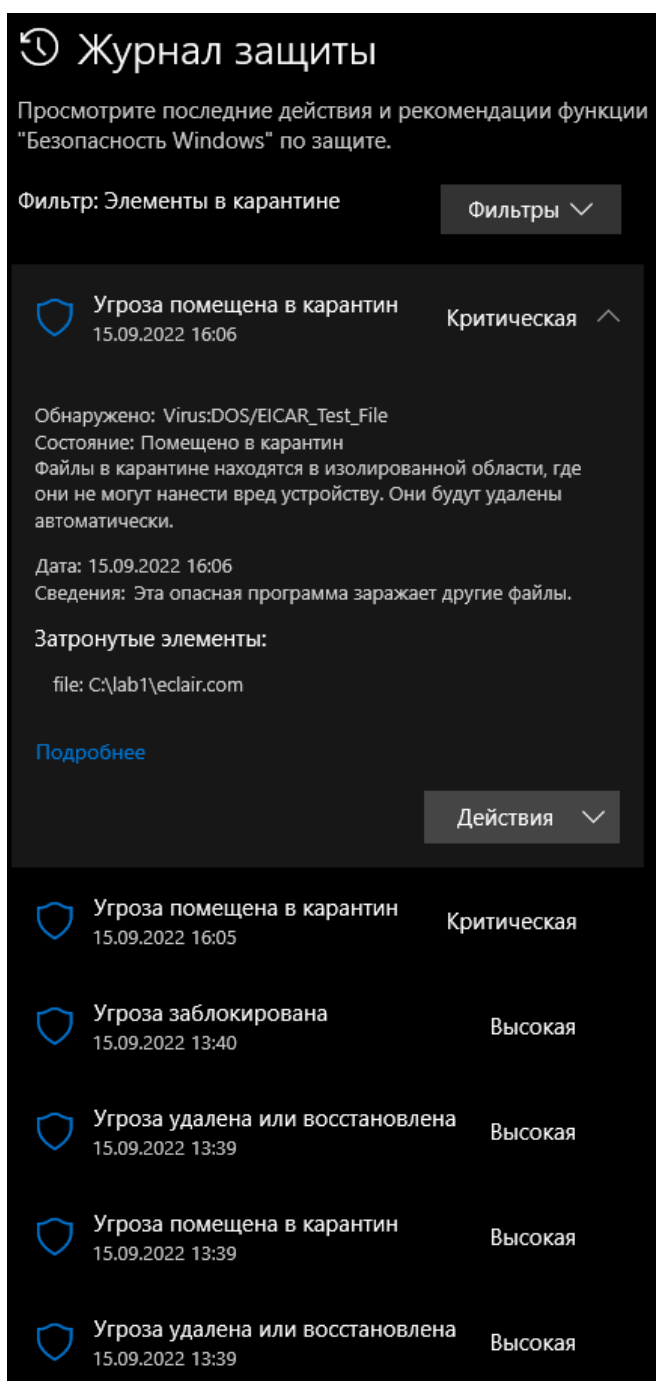
1.2 Добиться реакции антивируса на самописный вирус/детектируемую программу.

В качестве вредоносной программы был выбран KMSAuto NET 2022 (программа для активации windows). Windows Defender при проверке обнаружил угрозу, позволил запустить программу, но не воспользоваться ей.



1.3 Логи

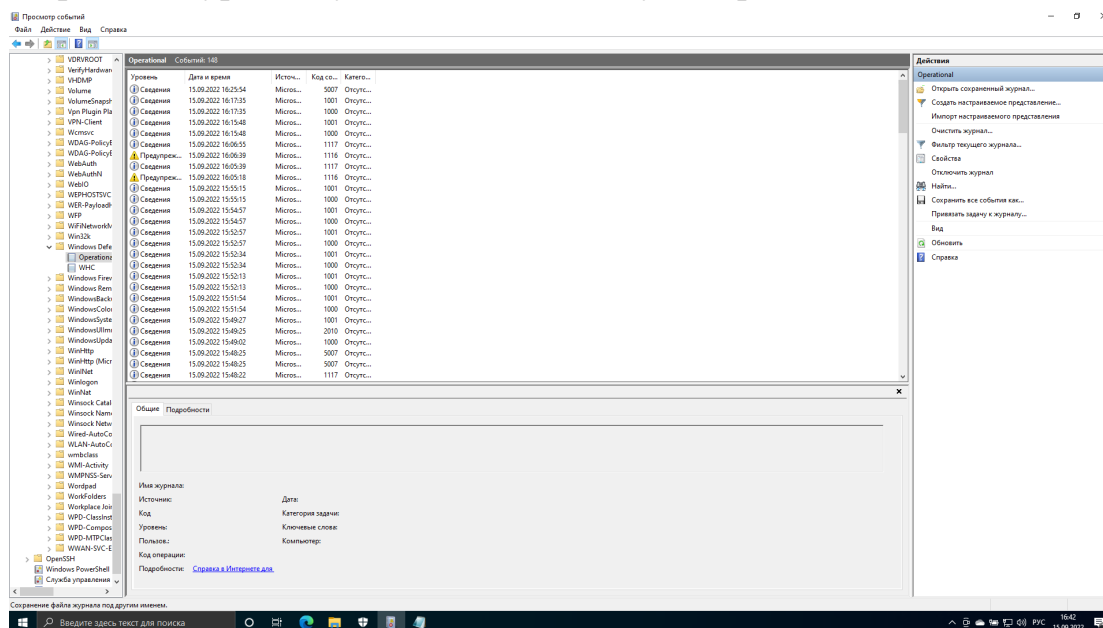
Вредоносная программа помещена в карантин. Через журнал защиты в Microsoft Defender можно убедиться, что в карантин помещены все файлы из папки.



Чтобы попасть в карантин через проводник, достаточно просто пройти по пути проводника «C:\ProgramData\Microsoft\Windows Defender\Quarantine». Все файлы в этой папке зашифрованы.

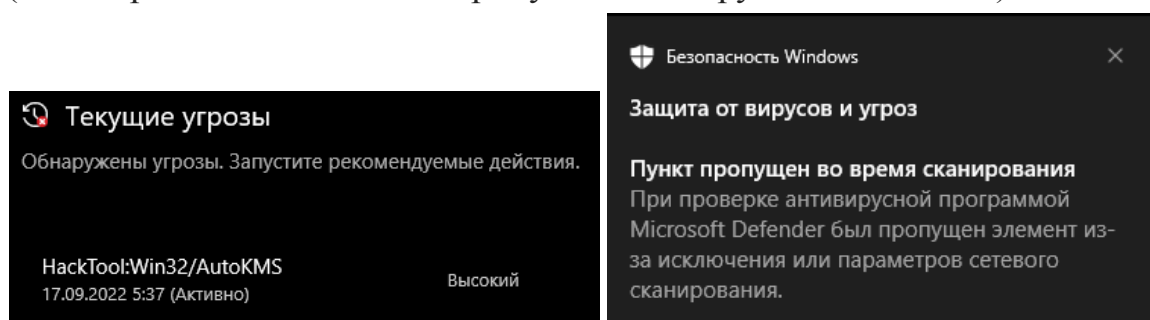
Чтобы посмотреть логи Windows Defender, нужно нажать “Win+R”, ввести в открывшееся окно eventvwr и проследовать по пути “Журналы приложений и

служб > Microsoft > Windows > Windows Defender > Operational”. Чтобы сохранить журнал, нужно нажать кнопку “сохранить все события как”.



Windows Defender оставляет в логах информацию о проведенных проверках, сменах своей конфигурации, отправке файлов в карантин и тд, в том числе, в случае обнаружения угроз, указывает имена вредоносных программ и процессов.

1.3 Папка с вредоносной программой помещена в исключения Windows Defender, в результате чего при проверке вредоносный файл был обнаружен (несмотря на оповещение о пропуске антивирусом этой папки).



1.4 На скачивание и распаковку архива ([metasploit-framework/modules/exploits/windows/smb](https://www.metasploit-framework.com/modules/exploits/windows/smb)) Windows Defender никак не отреагировал. При сканировании вручную реакции также не было.

2. Kaspersky Internet Security

2.1 Вирусные базы обновлены, при быстрой проверке системы угроз не обнаружено.

Базы актуальны

По умолчанию Kaspersky Internet Security автоматически проверяет наличие пакета обновлений на серверах обновлений "Лаборатории Касперского", скачивает и устанавливает его в фоновом режиме. Вы можете в любой момент запустить обновление баз и программных модулей вручную.

Обновить

Последнее обновление: 1 минуту назад



Безопасно: угроз не обнаружено.

Быстрая проверка завершена меньше минуты назад

✓ Проверено 3 044 файла.

2.2 После скачивания вредоносной программы быстрая проверка обнаружила угрозы и предложила их устранить. При попытке запустить вредоносную программу антивирус заблокировал это действие.

Защита

	C:\ProgramData\KMSAutoS\KMSAuto Net.exe Обнаружена вредоносная утилита. Время: 16.09.2022 19:38	Устранить ▼
	C:\Users\aeshe\Downloads\k... 2016 v1.5.4 Portable\KMSAuto Net.exe Обнаружена вредоносная утилита. Время: 17.09.2022 5:28	Устранить ▼

❗ Сегодня, 17.09.2022 5:29:25 Процесс завершен

Событие: Процесс завершен
Программа: KMSAuto Net
Пользователь: DESKTOP-RGKF4BA\aeshe
Тип пользователя: Активный пользователь
Компонент: Мониторинг активности
Описание результата: Завершен
Тип: Упакованная программа, которая может нанести вред
Название: not-a-virus:PDM:HackTool.Win32.Yzon.a
Степень угрозы: Средняя
Тип объекта: Процесс

Первый файл успешно вылечен антивирусом без помещения в карантин, второй добавлен в исключения.

Обнаружено: HackTool.MSIL.HackKMS.gen
Расположение: C:\Users\ae...Portable\KMSAuto Net.exe
Не удастся вылечить обнаруженный объект.

Удалить

Пропустить

Добавить в исключения

2.3 После добавления вредоносного файла в исключения проверка обнаружила его как угрозу и предложила варианты устранения проблемы.

Внимание: 1 объект не вылечен.

Быстрая проверка завершена меньше минуты назад

1 объект не обработан.

2.4 При сканировании папки со скачанным архивом ([metasploit-framework/modules/exploits/windows/smb](#)) Kaspersky не обнаружил угроз.

2.5 Логи установки или удаления программ хранятся в папке %USERPROFILE%\AppData\Local\Temp

В ней обнаружена папка пустая Temp1_kmsautonet.zip\kmsautonet.

Журнал событий (отчет файлового антивируса в текстовом виде приложен в конце отчета о лабораторной работе):

Файловый Антивирус

Обновить Сохранить отчет

Важность: Поиск

Время: День < 17.09.2022 17.09.2022 >

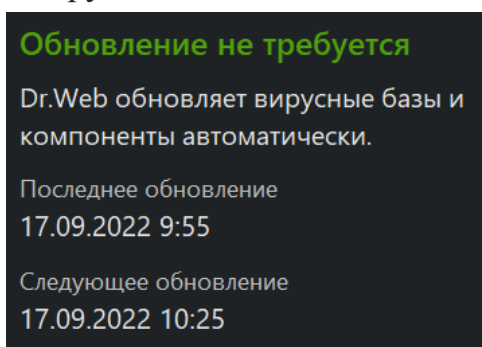
Дата события	Объект
! Сегодня, 17.09.2022 6:02:31	C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net
! Сегодня, 17.09.2022 6:02:31	C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net
! Сегодня, 17.09.2022 6:01:24	C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net
! Сегодня, 17.09.2022 6:01:24	C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net
! Сегодня, 17.09.2022 5:44:49	
! Сегодня, 17.09.2022 5:35:39	
! Сегодня, 17.09.2022 5:32:01	

! Сегодня, 17.09.2022 6:02:31 Лечение невозможно

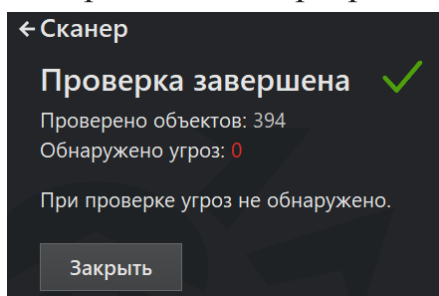
Событие: Лечение невозможно
Пользователь: DESKTOP-RGKF4BA\aeshe
Тип пользователя: Активный пользователь
Имя программы: smartscreen.exe
Путь к программе: C:\Windows\System32
Компонент: Файловый Антивирус
Описание результата: Не обработано
Тип: Программа, которая может нанести вред
Название: HackTool.MSIL.HackKMS.gen
Точность: Частично

3. Dr. Web

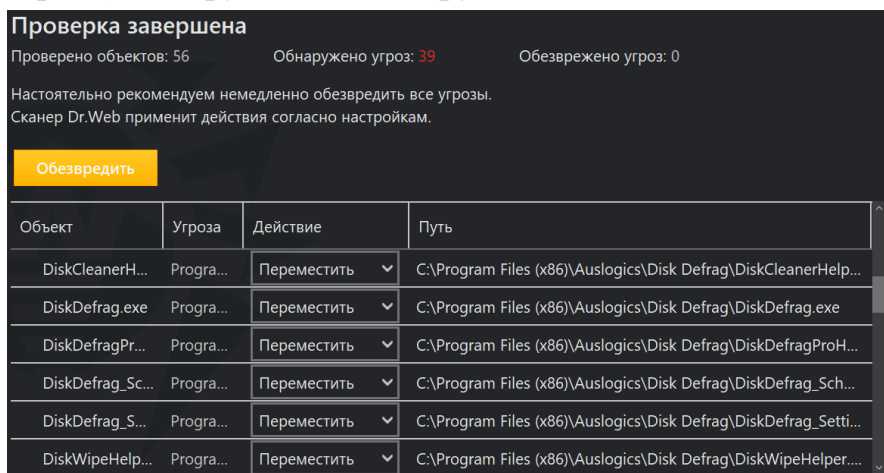
3.1 Вирусные базы обновлены, при быстрой проверке системы угроз не обнаружено.



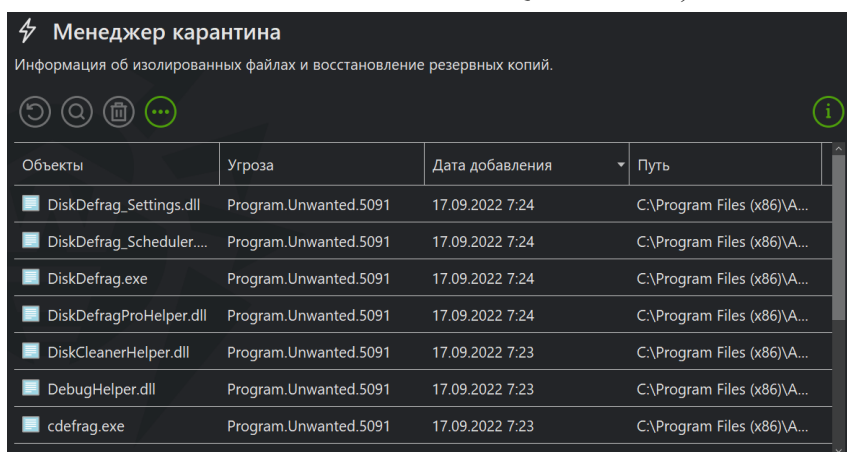
3.2 Вредоносная программа KMS Auto Net антивирусом не обнаружена.



Другая вредоносная программа Auslogics Disk Defrag (нелицензионная версия) обнаружена антивирусом



3.2 Все вредоносные файлы помещены в карантин (путь к папке карантина: %USERPROFILE%\DoctorWeb\Quarantine\)

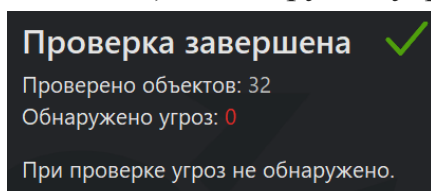


3.3 После добавления папки с вредоносной программой в исключения антивирус не обнаруживает угроз при проверке.

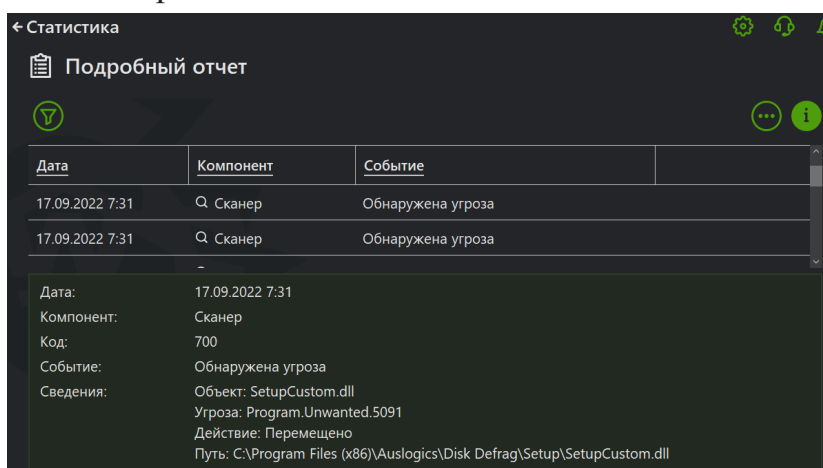
3.4 При скачивании архива всего проекта с гита (<https://github.com/rapid7/metasploit-framework>) Dr. Web регистрирует архив как вредоносный и не позволяет совершить с ним действий, например, разархивации.










При скачивании и проверке только указанной папки (<https://github.com/rapid7/metasploit-framework/tree/master/modules/exploits/windows/smb>) антивирусом угроз не обнаружено.



Dr. Web предоставляет отчет о всех действиях.



Логи Dr.Web расположены по адресу “C:\ProgramData\Doctor Web\Logs”,
открыть можно только от имени администратора.

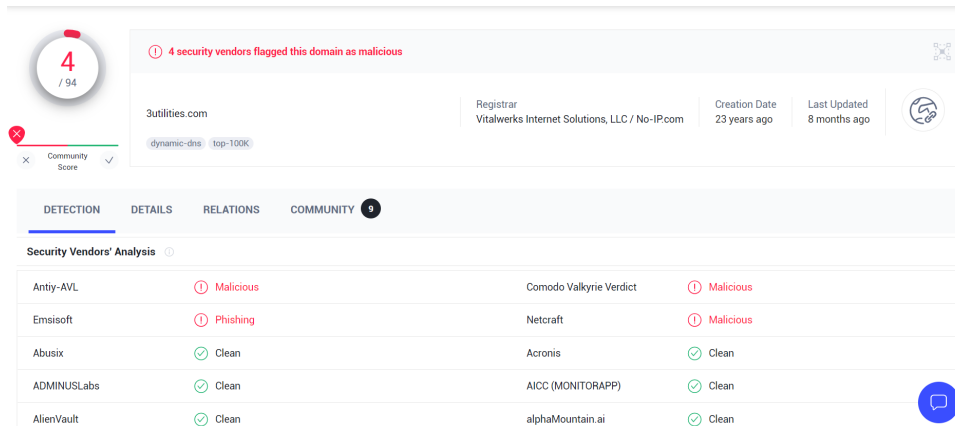
 distrib-starter	17.09.2022 6:57	Текстовый документ	10 КБ
 dwservice	17.09.2022 9:38	Текстовый документ	8 282 КБ
 dwupdater	17.09.2022 9:29	Текстовый документ	572 КБ
 netfilter	17.09.2022 9:37	Текстовый документ	489 КБ
 spiderg3	17.09.2022 9:37	Текстовый документ	9 594 КБ
 ss-setup	17.09.2022 6:57	Текстовый документ	653 КБ
 wsc-service	17.09.2022 9:37	Текстовый документ	20 КБ

4. VirusTotal

Сервис используется для анализа подозрительных файлов, доменов, IP-адресов и URL-адресов для обнаружения вредоносных программ.

Проверены 3 вредоносных домена:

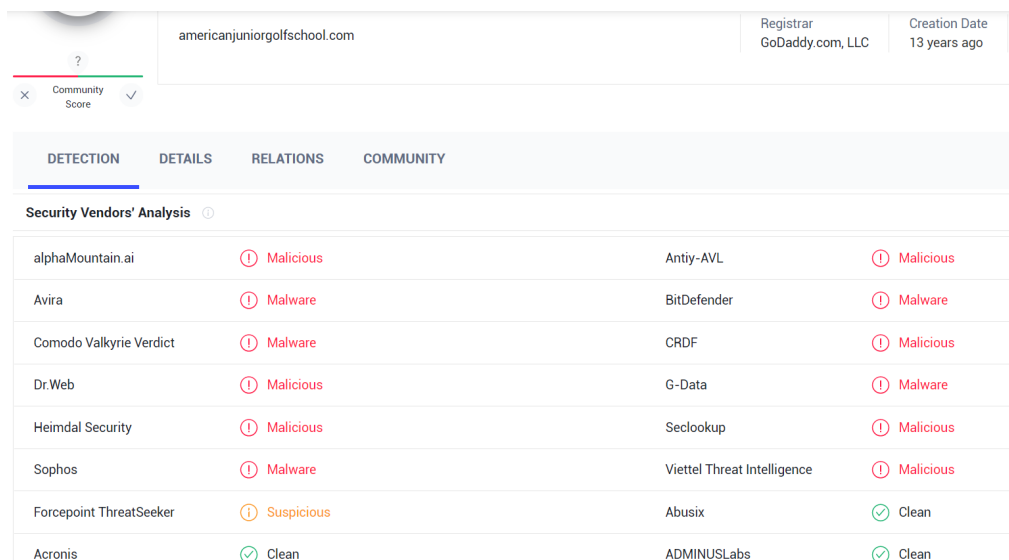
- 3utilities.com - замечен в спаме/фишинге по электронной почте
- americanjuniorgolfschool.com - вредоносный, согласно 12 источникам (включая Dr.Web)
- borcom.de - вредоносный, согласно 7 источникам (включая Dr.Web)



The screenshot shows the VirusTotal interface for the domain 3utilities.com. At the top, a circular badge indicates a score of 4/94. A warning message states: "4 security vendors flagged this domain as malicious". Below this, the domain name is listed along with its registrar (Vitalwerks Internet Solutions, LLC / No-IP.com), creation date (23 years ago), and last updated date (8 months ago). The "DETECTION" tab is selected, showing a "Security Vendors' Analysis" table with the following results:

Vendor	Verdict	Vendor	Verdict
Antiy-AVL	Malicious	Comodo Valkyrie Verdict	Malicious
Emsisoft	Phishing	Netcraft	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

3utilities.com domain reputation including recent account abuse & disposable email validation.



The screenshot shows the VirusTotal interface for the domain americanjuniorgolfschool.com. The domain name is listed along with its registrar (GoDaddy.com, LLC) and creation date (13 years ago). The "DETECTION" tab is selected, showing a "Security Vendors' Analysis" table with the following results:

Vendor	Verdict	Vendor	Verdict
alphaMountain.ai	Malicious	Antiy-AVL	Malicious
Avira	Malware	BitDefender	Malware
Comodo Valkyrie Verdict	Malware	CRDF	Malicious
Dr.Web	Malicious	G-Data	Malware
Heimdal Security	Malicious	Seclookup	Malicious
Sophos	Malware	Viettel Threat Intelligence	Malicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

Did you intend to search across the file corpus instead? [Click here](#)

7
/ 94

?

Community Score

7 security vendors flagged this domain as malicious

borcom.de

DETECTION

DETAILS

RELATIONS

COMMUNITY

Security Vendors' Analysis

alphaMountain.ai	Malicious	Antiy-AVL	Malicious
Avira	Malware	Comodo Valkyrie Verdict	Malware
Dr.Web	Malicious	Heimdal Security	Malicious
Seclookup	Malicious	Forcepoint ThreatSeeker	Suspicious
Abusix	Clean	Acronis	Clean

Проверен один заведомо не вредоносный домен - google.com. Домен признан безопасным, согласно анализу всех вендоров средств безопасности.

At least 10 detected files communicating with this domain

0
/ 94

✓

Community Score

google.com

top-1K

Registrar
MarkMonitor Inc.

Creation Date
25 years ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 30+

Security Vendors' Analysis

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AICC (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Armis	Clean
Avira	Clean	BADWARE.INFO	Clean

Заключение

В данной лабораторной работе было изучено следующее антивирусное ПО: Windows Defender, Kaspersky Internet Security и Dr.Web, а также изучена работа сайта VirusTotal.

В рамках работы было проверено, как указанное ПО справляется с типовыми задачами антивируса: обнаружение вредоносных файлов, блокировка их работы, добавление файлов в исключения.

Windows Defender, обнаружив вредоносный файл KMSAuto, запуск файла не блокировал, но изменения в компьютер внести не позволил. KIS не дал запустить вредоносный файл KMSAuto. Dr.Web не обнаружил указанный вредоносный файл. Различия в возможностях обнаружения могут быть связаны с тем, что антивирусы используют разные вирусные базы.

В процессе своей работы все антивирусы ведут журнал событий. В эти журналы записываются действия антивируса, его состояние, а также названия вредоносных программ и пути к ним. На основе данных из таких журналов можно выяснить, какое вредоносное ПО устанавливалось и запускалось на компьютере.

На примере трех вредоносных/фишинговых доменов и одного безопасного проверена работа сервиса VirusTotal.

Приложение 1. Отчет файлового антивируса Kaspersky Internet Security.

Сегодня, 17.09.2022 6:02:31 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net.exe KMSAuto Net.exe

C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable Файл

Не обработано Лечение невозможно Не обработано

HackTool.MSIL.HackKMS.gen Программа, которая может нанести вред

Средняя Частично Windows Defender SmartScreen smartscreen.exe

C:\Windows\System32\smartscreen.exe C:\Windows\System32 9284

DESKTOP-RGKF4BA\aeshe Активный пользователь Пропущено

Сегодня, 17.09.2022 6:02:31 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net.exe KMSAuto Net.exe

C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable Файл

Обнаружено Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя Обнаружено HackTool.MSIL.HackKMS.gen

Программа, которая может нанести вред Средняя Частично Windows Defender SmartScreen smartscreen.exe

C:\Windows\System32\smartscreen.exe C:\Windows\System32 9284

DESKTOP-RGKF4BA\aeshe Активный пользователь Экспертный анализ

Сегодня, 17.09.2022 6:01:24 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net.exe KMSAuto Net.exe

C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable Файл

Не обработано Лечение невозможно Не обработано

HackTool.MSIL.HackKMS.gen Программа, которая может нанести вред

Средняя Частично Windows Explorer explorer.exe C:\Windows\explorer.exe

C:\Windows 6128 DESKTOP-RGKF4BA\aeshe Активный пользователь

Пропущено

Сегодня, 17.09.2022 6:01:24 C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable\KMSAuto Net.exe KMSAuto Net.exe

C:\Users\aeshe\Downloads\kmsautonet\KMSAuto Net 2016 v1.5.4 Portable Файл

Обнаружено Обнаружена легальная программа, которая может быть использована злоумышленником для нанесения вреда компьютеру или данным пользователя Обнаружено HackTool.MSIL.HackKMS.gen

Программа, которая может нанести вред Средняя Частично Windows

Explorer explorer.exe C:\Windows\explorer.exe C:\Windows 6128
 DESKTOP-RGKF4BA\aeshe Active user Expert analysis
 Today, 17.09.2022 5:44:49 Task started
 avp.exe C:\Program Files
 (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\avp.exe C:\Program Files
 (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3
 DESKTOP-RGKF4BA\aeshe Active user
 Today, 17.09.2022 5:35:39 Task
 stopped avp.exe C:\Program
 Files (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\avp.exe C:\Program
 Files (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3
 DESKTOP-RGKF4BA\aeshe Active user
 Today, 17.09.2022 5:32:01 Task started
 avp.exe C:\Program Files
 (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\avp.exe C:\Program Files
 (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3
 DESKTOP-RGKF4BA\aeshe Active user
 Today, 17.09.2022 5:26:32 Task
 stopped avp.exe C:\Program
 Files (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\avp.exe C:\Program
 Files (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3
 DESKTOP-RGKF4BA\aeshe Active user
 Today, 17.09.2022 0:40:30 Task started
 avp.exe C:\Program Files
 (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3\avp.exe C:\Program Files
 (x86)\Kaspersky Lab\Kaspersky Internet Security 21.3 NT
 AUTHORITY\SYSTEM System user